Дорожная карта «Сейфнет» — сквозные решения безопасности для рынков НТИ

Road map "SafeNet" end — to-end security solutions for NTI markets

Аннотация

В публикации представлено обсуждение рынка «Сейнет», необходимости его развития с целью предоставления защищенной инфраструктуры, обеспечения безопасности и доверенности всех рынков Национальной технологической инициативы. Обсуждены вопросы доверенности и безопасности кибер-физических систем в широком смысле, вопросы нормативного регулирования рынков НТИ и готовности решений Сейфнет к выходу на глобальные рынки.

Ключевые слова

Национальная технологическая инициатива, дорожная карта, Сейфнет, безопасность

Abstract:

The publication presents a discussion of the «SafeNet» market, the need for its development in order to provide new protected infrastructure, digital security applications and trustworthiness for all markets of the National technological initiative. There have been discussed issues of trustworthiness and security of cyber-physical systems, legal and technical regulation of NTI markets and the readiness of SafeNet solutions to enter the global markets

Key words:

National technology initiative, NTI, roadmap, SafeNet, trustworthiness, security

doi 10.26310/2071-3010.2019.253.11.008

В послании Федеральному собранию 4 декабря 2014 года Президент России Владимир Путин обозначил Национальную технологическую инициативу одним из приоритетов государственной политики. НТИ развивается на основе долгосрочного прогнозирования для решения задач по обеспечению национальной безопасности, качества жизни людей, развития отраслей нового технологического уклада. Особое место в структуре НТИ занимает рынок Сейфнет (SafeNet), который затрагивает работу всех других рынков НТИ, предоставляя им защищенную инфраструктуру и конкретные решения для снижения рисков и обеспечения безопасности. На публичной презентации дорожной карты Сейфнет, которая состоялась недавно в Санкт-Петербурге, в рамках проходившего мероприятия «Баркемп 20.35» шел разговор о необходимости развития этого рынка для поддержки всех дорожных карт НТИ, о вопросах доверенности и безопасности кибер-физических систем, нормативного регулирования рынков НТИ и готовности решений в этой сфере к выходу на глобальные рынки. **В обсуждении концепции дорожной карты приняли участие Валентин Макаров, президент НП «РУССОФТ», лидер рабочей группы Сейфнет Национальной технологической инициативы; Дмитрий Хан, аналитик Центра научно-технологического форсайта Университета ИТМО, координатор сегмента «Безопасные системы связи, обработки и хранения данных; Никита Уткин, председатель Технического комитета 194 «Кибер-физические системы»; Артур Глейм, начальник департамента квантовых коммуникаций ОАО «РЖД»; Денис Кувиков, директор по развитию бизнеса РИЦ «Сейфнет».** Все они являются членами рабочей группы, которые участвовали в актуализации концепции и дорожной карты Сейфнет.

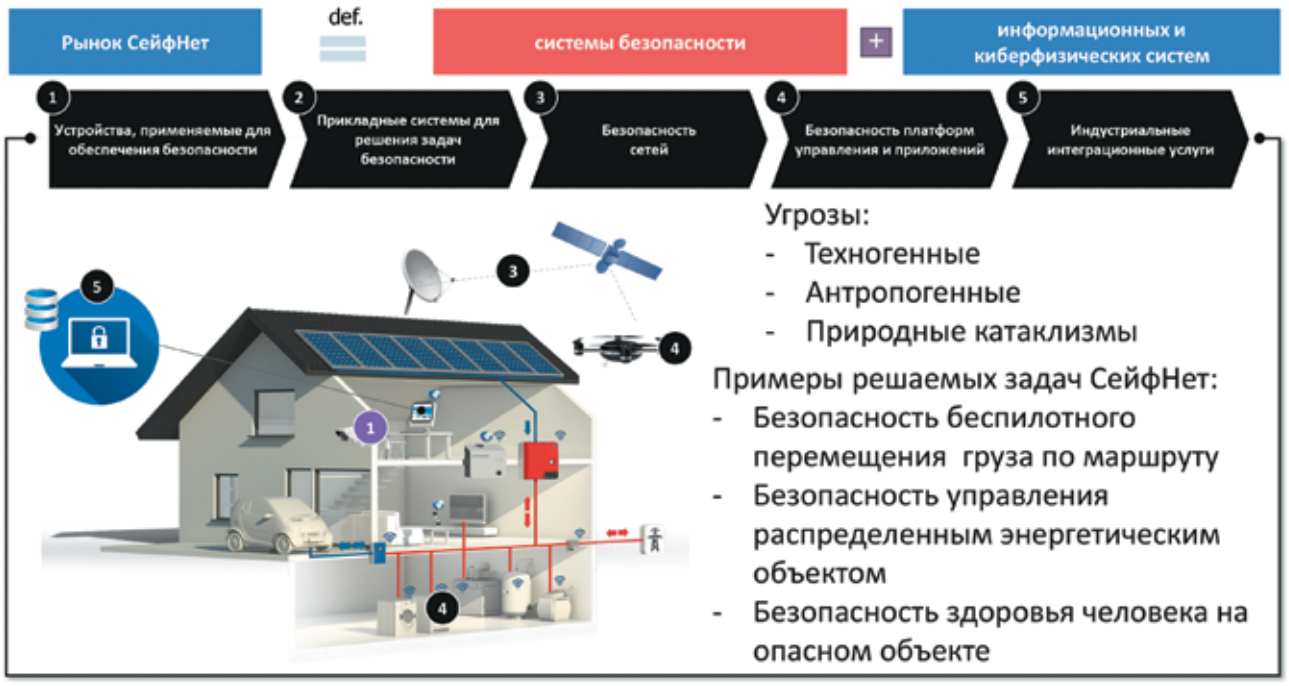
Валентин Макаров (Valentin Makarov)

Сейфнет — эта рабочая группа, которая занимается безопасностью информационных и кибер-физических систем. Мы находимся на этапе становления шестого технологического уклада, когда происходит процесс превращения систем автоматизированного управления критическими инфраструктурами, которыми управляет челочек, в системы, в которых человек выведен из контура управления, и сама кибер-физическая система управляет всеми своими процессами. Человек задает только правила игры и их корректирует. Важно то, что при переходе к кибер-физическим системам требования к безопасности меняются качественно, а все существующие сегодня меры защиты информации не будут соответствовать новым требованиям кибер-физического мира.

Кроме того, Сейфнет предоставляет конкретные решения по снижению рисков и обеспечению безопасности для каждого из «нетов» — причем для всех видов рисков — эндогенных, техногенных, антропогенных, рисков кибератак. В условиях перехода к кибер-физическим системам появляется требование новой парадигмы безопасности, включающей требования превентивности обеспечения безопасности, доверенности системы на всех этапах жизненного цикла, а также интеграции функции безопасности с самого начала проектирования как органической части кибер-физической системы. Нельзя сначала спроектировать беспилотный автомобиль, а потом придумывать, как его защитить от хакеров. Либо это не получится, либо будет слишком дорого.

На первом этапе разработки Концепции «Сейфнет» безопасность кибер-физических систем занимала умы членов Рабочей группы, но очень скоро мы все более отчетливее стали понимать, что человек является не менее ответственным объектом обеспечения безопасности. У нас есть целый ряд проектов, направленных на обеспечение безопасности человека — как информационной защищенности в цифровом мире, так и его физической безопасности. В частности, есть проект, который связан с возможностью обнаружения минимальных количеств взрывчатых веществ и может

| СейфНет — это рынок систем безопасности информационных и киберфизическихсистем



Примеры киберфизических систем[1]: *роботы, интеллектуальные здания, медицинские имплантаты, самоуправляемые автомобили, беспилотные самолеты ...*

1. Киберфизические системы – умные системы, включающие сети взаимодействующих между собой вычислительных и физических компонентов.

применяться в системах безопасности в аэропортах, на стадионах, в метро, в других местах скопления людей. Созданное в рамках проекта оборудование сертифицировано регулятором и одобрено к применению внутри страны, оно может стать нашим конкурентным лидером при выходе на глобальный рынок систем безопасности.

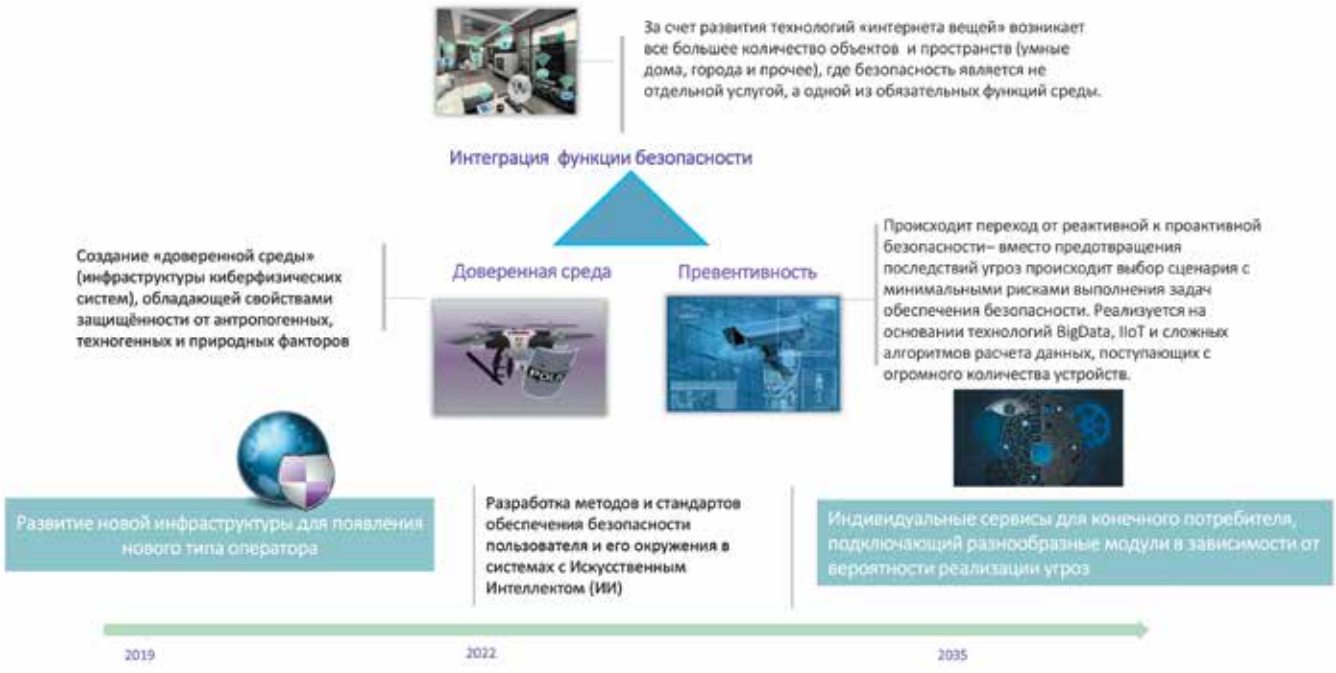
Второй проект, который появился совсем недавно, связан с глобальной системой мониторинга перемещения стрелкового оружия и боеприпасов к нему. Его реализация поможет расследовать преступления, которые часто являются трансграничными. Этот проект соответствует направленности НТИ, является примером решения глобальной задачи, которой позволит России стать технологическим лидером не только на территории Евразии, но и на других континентах.

Угрозы в кибер-физическом мире возникают от техногенных, антропогенных, природных факторов, и уже понято, что противодействовать им можно только применяя новую инфраструктуру безопасности и новые приложения, которые базируются на новых физических принципах. Только так можно гарантировать, чтобы дроны не падали на прохожих, никто бы не обстрелял нефтезаводы в Саудовской Аравии, «умный» дом внезапно не стал бы управлялся издалека третьими лицами и тому подобное — вот чем мы должны заниматься.

В рамках «Сейфнет» мы выработали новую парадигму безопасности кибер-физического мира, которая складывается из трех важных компонентов. Первый — это превентивность безопасности. Реактивный характер безопасности, какой человечество использует сейчас, для кибер-физического мира не подходит. А походит только превентивный, когда мы, имея возможность контролировать ситуацию, анализируем ее с помощью огромной сети датчиков разной физической природы, используя технологии обработки больших данных, искусственного интеллекта (ИИ), выявляем риски для выполнения порученной нам функции и выставляем такую траекторию исполнения этой функции, чтобы эти риски свести к минимуму. Превентивность — коренной фактор парадигмы безопасности.

Второй фактор безопасности, который не является очевидным для многих, — это доверенность среды, на которой мы строим систему безопасности. Долгое время считалось, что нет ничего страшного, если Россия будет использовать электронные компоненты Intel, программное обеспечение Oracle или других американских, английских или китайских компаний. Оказалось, что для кибер-физических систем это несправедливо. Необходимость применения доверенной среды неизбежна, но пока это понятие с трудом осознается теми, кто профессионально не связан с системами безопасности. Доверенное железо, доверенный софт, а также системы коммуникаций и средства проектирования и программирования того и другого тоже должны быть доверенными. Нельзя использовать как доверенные системы, созданные, например, в США.

I Путь к новой парадигме безопасности



Третий фактор — это интеграция функций безопасности в саму систему. Сегодня без интегрированной системы безопасности создать защищенную кибер-физическую систему нельзя. Например, нельзя сначала проектировать беспилотный транспорт и только потом взяться разработать систему его безопасности. При таком подходе регулятор не позволит использовать эту систему. Нужно закладывать требования к безопасности, проектируя саму систему. И во многом это спасает разработчика, поскольку он будет использовать средства программирования и проектирования с интегрированной функцией безопасности, что предотвращает нарушения требований безопасности при проектировании самой системы. Если применять такой подход, то можно более обоснованно обращаться к регулятору за получением его одобрения и сертификации созданной системы. Следствием этого является то, что мы подходим к тому моменту, когда без учета новой парадигмы безопасности регулятор никому не разрешит использовать беспилотный автомобильный, морской и воздушный транспорт, активную телемедицину, умную энергетику или распределенное цифровое производство. Такая практика будет применяться не только в России, но и во всем мире.

В концепции Сейфнет обозначены четыре основных области обеспечения безопасности. Во-первых, это создание доверенной среды для киберфизических систем, которая будет обеспечивать безопасное управление критической инфраструктурой энергетики, беспилотного транспорта, телемедицины, финансов и т. д. Во-вторых — создание системы безопасной передачи информации с использованием нового физического принципа ее защиты — квантового распределения ключей. В-третьих — обеспечение непрерывного биометрического контроля (идентификации и аутентификации) людей как пользователей услуг государственных, финансовых, медицинских и иных организаций, а также услуг кибер-физических систем. И в-четвертых — создание систем искусственного интеллекта для обработки больших объемов данных, оценки рисков и принятия решений с целью обеспечения безопасности функционирования кибер-физических систем, финансовых транзакций и транзакций с интеллектуальной собственностью.

Задачи, которые выполняет группа Сейфнет, следуя нашей дорожной карте — это достижение российскими компаниями на глобальном рынке доли не меньше 10%. И это возможно, учитывая достижения российских компаний, которые выходят на глобальные рынки систем безопасности. За последние три года из восьми российских компаний, которые вошли в символические «магические квадраты Гартнер» (мировой рейтинг производителей лучших программных продуктов) четыре компании действуют в области систем безопасности. У таких стран, как Южная Корея, Китай, Индия, Малайзия есть понимания того, что Россия является альтернативным источником разработок по кибер-безопасности. Уровень безопасности российских систем сравним с уровнем наших конкурентов — в первую очередь, из США, Великобритании и Израиля.

Взаимодействуя с разными дорожными картами НТИ, мы пришли к выводу, что без внедрения инфраструктуры и приложений безопасности Сейфнет ни одна рабочая группа НТИ (а все они сегодня работают с кибер-физическими системами), не сможет реализовать свои планы. Продукты, решения дорожной карты нашей рабочей группы являются необходимым базисом для того, чтобы все другие рабочие группы НТИ смогли успешно реализовать свои дорожные карты.

Этого понимания в широком смысле сначала не было почти у всех других рабочих групп. И их можно было понять, поскольку все рабочие группы старались преодолеть свои технологические барьеры, особенно не имея ни времени, ни желания обсуждать проблемы безопасности. Сегодня такое понимание есть. Сейчас мы начинаем готовить для Автонет инфраструктурные решения, которые помогут обеспечить безопасность беспилотного транспорта по маршруту из Юго-Восточной Азии через территорию России и Казахстана дальше в Европу. Для решения такой масштабной задачи нужно развивать технологии безопасности человека и кибер-физических систем. Мы сравнили дорожные карты других рабочих групп НТИ, их основных направлений деятельности, и оказалось, что практически в каждой из них есть отдельные блоки безопасности, интегрированные в нашу дорожную карту, как подтверждение того, что Сейфнет создает инфраструктуру и приложения для полноценной работы всех других рабочих групп.

Дмитрий Хан (Dmirii Han)

Я расскажу о нашем подходе к формированию дорожной карты

Рынок Сейфнет 2035

и в целом к проекту Сейфнет с рыночной точки зрения и тех требований по безопасности, которые рынок и новая индустрия, новые сервисы предъявляют к киберфизической инфраструктуре. Мы понимаем, что сегодня цифровизуются финансы, инфраструктура, логистика, железные дорога т. д. Объем данных растет, соответственно под эти данные нужны сервисы, которые данные сохранят, обработают и передадут потребителям. В связи с этим на рынок выходят новые компании из IT-сферы. Те классические отрасли, которые раньше обслуживались банками, корпорациями, сегодня начинают обслуживаться инфраструктурой. Такие гиганты как IBM, AMAZON и другие корпорации имеют огромную клиентскую базу, разветвлённую сеть каналов связи по всему миру. Они планируют занять не менее 10% обслуживания финансовых транзакций в мире за счет того, что будут переводить их на свою собственную инфраструктуру и в принудительно-добровольном порядке обслуживать своих контрагентов, поставщиков, клиентов внутри замкнутой инфраструктуры платежей. При этом, финансовая транзакция не отличается от любой другой цифровой транзакции, так что эти тенденции будут наблюдаться и в других отраслях.

С точки зрения безопасности формирования новой инфраструктуры невозможно вырастить небольшой стартап, не создав под него набор стандартов и сопутствующих решений, которые обслуживали бы в дальнейшем сервисы безопасности. Таким образом, второй подход к дорожной карте связан с тем, что мы работаем с перспективными рынками, мы пытаемся работать со стандартами, которые появляются на базе тех технологических решений, которые есть внутри экономики Сейфнет.

Наконец, можно говорить о нескольких уровнях, с которыми мы работаем. Первый уровень — физический, при котором нужно обеспечить безопасность физических характеристик при передаче, хранении и обработке данных в центрах обработки данных (ЦОДах) и т. д. В этом направлении мы работаем с такими технологиями как квантовое распределение ключей, защищенные ЦОДы, доверенная вычислительная техника и коммуникационная аппаратура и др. Второй уровень — транзакционный, то есть, обеспечение транзакций взаимодействия цифровых агентов в сети. Что это означает? В ближайшее время физические перемещения тех или иных объектов — беспилотного транспорта, мобильных устройств, людей скорее всего будут привязаны к той инфраструктуре, которая обеспечивает включенность этих устройств в доверенную сеть. Например, беспилотные автомобили будут ездить вдоль тех дорог, которые обслуживаются безопасной кибер-физической инфраструктурой: датчиками, оптоволокном, ЦОДами, которые соответствуют тем стандартам, которые принимают крупные корпорации или государство. Далее это приведет к тому, что страхование и ответственность за грузы будут привязаны к тому, включен или нет страховой агент в доверенную сеть. Если, например, в России какое-то пространство не встроено в без-

опасную инфраструктуру, соответствующую мировым стандартам безопасности, размер страховки может значительно увеличиться по сравнению с другими странами, выполняющими это условие.

Это еще одно обоснование того, почему мы пытаемся работать со стандартами, согласовывать их с нашими международными партнерами. Собственно, это же определяет выбор набора сервисов, связанных с транзакциями. Один из наших проектов — безопасная транзакционная финансовая инфраструктура для Евразийского пространства, как раз связана с тем, что за финансовый рынок сегодня начинают бороться крупные корпорации, которые наравне с крупными банками выстраивают свои платежные инфраструктуры для обслуживания товарооборота между странами. Сегодня контроль за кибер-физической инфраструктурой ведет к контролю финансовых и товарных потоков.

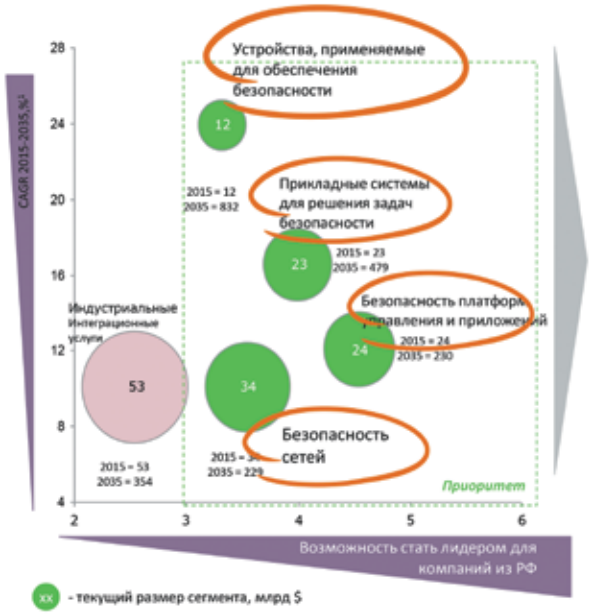
Мы формируем собственные стандарты и дальше будем выстраивать определенные сервисы для того, чтобы контролировать товарные потоки и финансовые транзакции, соответственно здесь идет сопряжение второго уровня физической инфраструктуры с инфраструктурой транзакционной, с технологиями распределенных реестров, обработкой данных и т. д., что позволяет в режиме реального времени совершать безопасный обмен данными, финансовыми транзакциями. Этому посвящен Евразийский проект общего транзакционного финансового пространства.

Более высокий уровень требований связан с тем, чтобы выстраивать сервисы для конечного потребителя. Здесь может возникать набор сервисных компаний, организация стартапов, которые, уже имея набор стандартов, могут встраиваться в международные сервисы. Соответственно с точки зрения продвижения этих проектов на международных рынках в рамках рабочей группы Сейфнет у нас выстроено несколько направлений формирования физической инфраструктуры. Во-первых, Евразийский квантовый путь. Пред-

Никита Уткин (Nikita Utkin)

ставители России от Сейфнет сейчас официально участвуют в нескольких международных группах по квантовым коммуникациям для того, чтобы согласовать движение данных из Европы в Азию по безопасному каналу. С точки зрения классической финансовой инфраструктуры идет согласование международной платежной системы, построенной на распределенных реестрах. Такое решение позволяет выстраивать независимые от каждого игрока

Приоритетные сегменты для ДК Сейфнет



Приоритетные сегменты для ДК Сейфнет

1 Устройства, применяемые для обеспечения безопасности

- Наиболее крупный сегмент с прогнозируемым **размером ~830 млрд.$** к 2035 году
- Существующая сильная **база научных разработок и специалистов** в РФ, наличие решений мирового уровня

Примеры: камеры видеонаблюдения со встроенным процессором, стерео-камеры для определения расстояния до объекта, датчики состояния здоровья пациентов

2 Прикладные системы для решения задач безопасности

- В РФ существует **лидирующая школа криптографии и биометрического контроля, наличие решений мирового уровня**

Примеры: рейтинг №1 в мире по распознавания голоса, системы идентификации человека по двум биометрическим параметрам (голос + изображение), 5 компаний входят в рейтинги ведущих мировых производителей систем безопасности

3 Безопасность сетей

- Наличие **сильных специалистов** в алгоритмистике, квантовых коммуникациях, фотонике и математике

Примеры: успешное проведение испытаний передачи ключей шифрования по квантовому каналу, разработаны **собственные архитектуры и стандарты** перспективной связи на новых физических принципах

4 Безопасность платформ управления и приложений

- В сегменте представлены **компании – мировые лидеры** из РФ. Высокий уровень **специалистов по кибербезопасности и архитектуре безопасных вычислений**

Примеры: **Лаборатория Касперского, МЦСТ**

транзакционные системы, то есть, в системах каждый игрок может с одной стороны предлагать правила игры, с другой — контролировать транзакции, распределенные между множеством игроков.

Чего же не хватает при работе над международными и национальными стандартами? И что нужно в национальном регулировании? В каком качестве мы можем выступать при разработке международных стандартов?

Дмитрий Хан: На текущий момент мы представлены на международных площадках, как участники международных рабочих групп со всеми правами экспертов, соредакторов. Но проблема в том, что для того, чтобы участвовать полноценно на международных площадках в качестве соредакторов, нужно активно отстаивать собственное понимание стандартов в этом сегменте. У нас таких ресурсов нет — получается борьба инициативы одного конкретного человека против всего мира.

Никита Уткин: Проблема номер один — не обеспечена финансовая поддержка участия российских экспертов в отстаивании интересов российских разработчиков в международных организациям в области стандартизации. Вторая проблема — не отработаны механизмы на национальном уровне в поиске консенсуса в формировании единой позиции, хотя механизмы есть — технические комитеты 194, 26, другие структуры. На мой взгляд, нужна единая площадка обсуждения, механизм интеграции усилий.

Дмитрий Хан: Несмотря на то, что в России работа по перспективным национальным стандартам ведется, ее нужно достаточно быстро гармонизировать с международными стандартами. Это не быстрый путь, достаточно времени займет и перевод действующих документов. Но это проактивная позиция. Второе, поскольку мы говорим о связанных с политикой технологиях, встроенных в концепцию доверенной среды, нет официально утвержденных документов консенсуса, которые бы позволили на них официально ориентироваться. Технологии по сути стандартизируются сами по себе, исходя из интересов локальных участников.

Никита Уткин: Я верю в саморегулирующийся рынок. Есть документ –нормативная дорожная карта, обозначенная в официальных документах, как дорожная карта по совершенствованию законодательства и устранению административных барьеров. Возможно, и в рамках рынка Сейфнет нужно идти на опережение в попытке решать проблему регулирования. Создать нормативную рабочую группу, куда бы входили как представители рынка, так и все необходимые регуляторы, с целью ускоренной разработки технических стандартов и формированию полноценной экосистемы нормативного регулирования, ориентированной на развитие.

Дмитрий Хан: Те эксперты и компании, которые участвуют в международных рынках по разным программам, продвигают не просто какие-то стандарты, а конкретные технические решения, исходя из своих интересов, и захватывают как национальные, так и глобальный рынки, понимая, что у них уже есть план по разворачиванию производств и экспансии на международные рынки. Необходимо при этом учитывать, что эти технологии между собой взаимосвязаны и сразу гарантируют комплексный выход на рынки распределенных реестров, 5G, новых систем связи, беспилотного транспорта и т. п. С пулом этих технологий они будут выходить, в том числе, и на российский рынок. На уровне глобального рынка мы начинаем проигрывать и отставать с точки зрения разработки стандартов и их продвижения.

Артур Глейм (Artur Gleim)

Давайте представим, что цифровая экономика случилась. Задачи выполнены и все цели ее достигнуты. Подсчитаем, какой объем защищенного трафика нужен, чтобы обеспечить цифровую экономику, защитить критические инфраструктуры, персональные данные. Как минимум 90% задачи цифровой экономики требует специальных средств обеспечения безопасности. Современные инфраструктуры, не говоря уже о безопасности, не обеспечивают пропускной способности этих систем. Сюда ложится вторая проблема — откуда взять такой объем защищенных каналов? Таким образом, проблема создания новых технологий и развития новых рынков является одним из ключевых драйверов новой экономики. Какие барьеры и какие задачи стоят для выхода на рынки формирования инфраструктуры?

Первый аспект- это технологический. Это запрос рынка на те задачи и решения, которые соответствуют технологии квантового распределения ключей. Первые решения начали появляться в 2000 году. Но только сейчас начали строить сети и приступать к их практическому применению. Это обоюдный процесс потребностей рынка и осознание их с точки зрения новых технологий.

Объективное развитие технологий с учетом тех компетенций, которые есть в стране и спрос глобального рынка в технологической потребности сходятся в единое целое.

Дальше есть два варианта. Первый — компании выполнят те задачи, которые прописаны в национальных программах (в Сейфнете) и решат ряд проблем, касающихся нормативного фактора — сферы нормативно регулируемой. Она регулируемая, потому что дает качество, но скорость регуляторики должна соответствовать скорости развития технологий. Это хорошо, но недостаточно.

Второй — создав отечественные технические решения, наши компании используют эти технологии для экспортных продуктов, экспорта идей на мировой рынок. И это потребует отстаивание интересов национальных производителей на глобальном рынке, так как российский рынок как мы понимаем ограничен. Современный мир устроен так, что имея только российский рынок, быть глобальным игроком невозможно. Вопрос глобализации российских компаний связан с международными рабочими группами и с международными стандартами, с конкурентами в лице глобальных корпораций, у которых огромный опыт в освоении глобального рынка, с огромными финансовыми ресурсами и политической мощью своих государств для защиты их интересов. На данный момент в России ввиду стартовой точки зарождающегося квантового рынка компаний с таким ресурсом де факто нет. Но есть задачи, которые нужно решать. В мире такие задачи решаются господдержкой и правильной консолидацией участников рынка и участников этого процесса. Соответственно, если первое и второе сделано, получается результат.

Первый опыт у нас уже есть. Сообщество разработчиков и производителей технологии квантовой коммуникации выдвинуло единого кандидата на представление интересов Российской Федерации в международную рабочую группу по квантовым коммуникациям. Теперь у нас есть свой рупор, и предложения российского представителя будут услышаны.

Практика показывает, что необходима правильная международная кооперация. Идет острая геополитическая борьба между США и Китаем. В сфере коммуникаций мы это сразу чувствуем. Если раньше российская технологическая база не интересовала Китай, то сейчас наоборот. В этом смысле геополитическая конфигурация складывается в пользу России, у которой есть мощнейший технический задел и есть пока еще не занятый собственный рынок, который находится на стадии стартового формирования. Есть правильно сложившаяся глобальная среда, способствующая этому процессу. Есть правильная геополитическая среда, определяющая те рыночные перспективы, которые у нас есть. Есть запросы о создании квазимонополий — картелей из российских разработчиков и производителей при поддержке государства с целью завоевания внешнего рынка.

Денис Кувиков (Denis Kuvikov)

Два года назад при поддержке правительства Санкт-Петербурга был создан РИЦ «Сейфнет», как инструмент, позволяющий тестировать на пилотных объектах разные конфигурации безопасности. Это абсолютно необходимый проект по значимости сопоставимый с тем, что есть в Китае и других странах, где уже приступили к новым технологиям будущего. На данный момент устройства квантового распределения ключей прошли испытания в ряде гос.организаций и к корпораций, включая Россети, ФСО, Ростелеком. В 2019 году в пилотную сеть были объединены две технологии — распределенного реестра и квантового распределения ключей — в единое кольцо по топологии сети. Имитирована атака хакеров на каналы, о чем мы показывали в СМИ. И в этой операции участвовали все значимые коллеги: Ростелеком, Квanттелеком, Т8, Супертел. Испытания прошли успешно, тем самым показав правильный путь, который мы проделали с нашего старта. Город сделал очень правильный шаг, создав этот центр. Сегодня ведутся испытания новых систем безопасности, проверяются гипотезы. Подключаются разные игроки, в том числе, такой крупный как РЖД, другие структуры, которые заинтересованы в безопасной передаче данных. Поскольку РИЦ «Сейфнет» — структура Технопарка «Санкт-Петербург», идет работа с молодыми командами, являющимися резидентами Технопарка. В перспективе мы должны видеть проблемы, связанные с сильной зарегулированностью этого рынка. И при таких условиях для новых игроков со свежими идеями ситуация усложняется.

Наше дальнейшее видение — усиливать объединение игроков, донести до всех лиц, принимающих решение, понимание того, что Сейфнет — это линия, проходящая через

все рынки НТИ, потому что ни один рынок НТИ без безопасности информации и инфраструктуры существовать однозначно не сможет. Пока мы работаем на энтузиазме и ответственности.

Очень важен вопрос законотворчества. Мы участвуем в различных экспертных сообществах, в том числе, при Госдуме РФ. Созданы проекты некоторых законов, которые предусматривают создание пилотных экспериментальных зон в виде регуляторных «песочниц», и отрабатываются вопросы квантового блокчейна. Наша задача — превратиться в реальный полигон федерального уровня по испытанию технологий безопасности.

Дмитрий Хан: В технологию квантовой коммуникации вкладываются не только государство, университеты, есть частные инвестиции и вполне приличные деньги. Если говорить про инжиниринговые центры, то они создавались как полигоны новых технологий с одной стороны, с другой как определенное экспертное сообщество, которое за технологиями видит рынок и решения, которые можно продавать. Ситуация противоречивая: средства частных инвесторов вкладываются на свой страх и риск, но регулятор тормозит процесс, а для частных денег это большой риск. На мой взгляд, нужны некоторые промежуточные инструменты, которые бы позволяли независимому сообществу, независимым площадкам, полигонам, внедренческим зонам быстрее апробировать те или иные новые решения. Возможно, такие дополнительные инструменты требуют дополнительной институализации, возможно, придать вес РИЦ Сейфнет, если не как сертифицирующему центру, но как месту, где можно официально протестировать решения на соответствие требованиям регулятора.

Артур Глейм: Мне кажется, Дмитрий высказал правильную идею. Можно воспользоваться опытом Минобрнауки, который использует функции монитора не только как контролера, но как партнера, помогающего исполнителю «сделать работу хорошо». И в этом смысле вопрос идеологический — какой запрос разработчики и экономика должны дать регуляторике, чтобы она выполняла не только барьерную функцию, но и содействовала разработчикам сделать все хорошо и быстро дойти до качества, после которого регулятор может выдать разрешение. И в этом концептуальная разница. Сейчас мы довольно много и плотно работаем с регулятором. Для всех компаний, глубоко интегрированных в этот процесс, и для тех, кто только начинает работать, это выглядит так, что есть забор и есть попытка его пробить, только с обратной стороны. На мой взгляд, если бы идеология могла бы меняться, либо появились дополнительные функциональные единицы, задачей которых был бы не только контроль, но помощь в том, чтобы барьер пройти. Тогда все сдвинется намного быстрее.

Реализованные или запущенные проекты Сейфнет, требующие поддержки для масштабирования

Инжиниринговый центр для отработки и внедрения прототипов ключевых решений СейфНет. Сборка и испытание прототипов киберфизических платформ.
Результат: запущен центр в СПб с 3 ЦОДами, защищенными квантовыми коммуникациями, и с развернутыми решениями и прототипами «доверенной среды». Функционирует в боевом режиме, предоставляет коммерческие услуги

Комплекс доверенных и безопасных средств и решений на основе российских технологий с реализацией международных стандартов для построения доверенных индустриальных комплексов на основе Интернета Вещей.
Результат: создание защищённых программно-аппаратных комплексов, предназначенных для критически важных промышленных систем.
2017-2020

Создание систем управления распределенными ЦОДами, защищенных квантовыми коммуникациями.
Текущий результат: региональные сети, запуск работы над российским стандартом, рост частных инвестиций

2018-2021

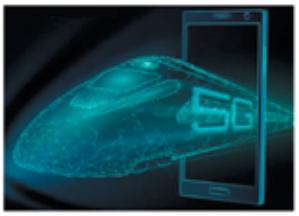
Создание национальной платформы для хранения, контроля и обмена биометрическими данными
Результат: прототип системы национального уровня для непрерывной идентификации личности по двум и более биометрическим параметрам

2018-2019

Значимые проекты с результатами в ближайшем времени обладают первостепенной важностью для поддержки в рамках НТИ

Независимая трансграничная платежная среда в ЕАЭС, БРИКС с многоконтурной инфраструктурой расчетов, с использованием распределенных реестров и в защищенном контуре.
Результат: прототип глобальной транзакционной платформы, пилотные сделки и проекты

2018-2021



Доверенная платформа, основанная на доверенных активных компонентах, системном и прикладном ПО, защищённая квантовым распределением ключей.
Применение – защищенная система 5G, вычислительные системы повышенной надежности для критической инфраструктуры и киберфизических систем, «Квантовый Интернет»

Создание современных защищенных систем обмена данными, контроля и мониторинга на всем жизненном цикле изделий в процессе производства, в торговле, на транспорте, в логистике, в учете товаров и услуг

Формирование и запуск комплексных проектов доверенной киберфизической среды на базе технологий и решений Сейфнет в странах ЕАЭС, БРИКС и в партнерстве с корпорациями (Росатом, РЖД, Глонасс).
Гармонизация стандартов IoT, ITS, QKD, NFV, DLT, с международными органами ETSI, ITU, ISO.

2019-2021

Никита Уткин: На мой взгляд, хорошее предложение. Это должно работать при условии того, что инициативы в области нормативного регулирования запускаются не для того, чтобы макулатуру сдать для отчета, а для того, чтобы решение пошло в рынок. На примере нашего опыта в области интернета вещей, могу сказать, что все разрабатываемые и утвержденные стандарты и протоколы в процессе разработки и публичного обсуждения проходили полную верификацию, мы их тщательно проверяем и дорабатываем совместно с регулятором в рамках действующих соглашений. На выходе получается не просто интересная доморощенная технология, а технология со знаком качества, верифицированная регулятором. Вопросы могут появиться на фазе апробации. В итоге мы получаем технологию задокументированную, разумную и прозрачную — технологию, в которой так или иначе отражены предложения регулятора. Например, криптографический блок в разработанными нами стандартах практически в каждом случае экспоненциально повышался в качестве.

Почему так происходит — не секрет. Блок доверенности и безопасности зачастую игнорируется разработчиками в своих решениях, и не в последнюю очередь, потому что инвестор хочет быстрых результатов, хотя за качество потом приходится краснеть именно разработчику. И это не только российская, это международная специфика. Когда мы закладываем технологию в стандарт, у нас есть уникальная возможность вместе с регулятором — не как с оппонентом, а как с союзником и партнером доработать эту технологию и вывести ее на новый уровень, открыть ее рынку.

P.S.

Любопытна и поучительна история рабочей группы и концепции «Сейфнет». Все документы были готовы к утверждению Межведомственной рабочей группой (МРГ) при правительстве еще в 2016 г., но по разным причинам они так и не были приняты по настоящее время. С одной стороны, отсутствие утвержденного статуса не позволило Рабочей группе получить доступ к финансовым источникам НТИ и к мерам административной поддержки.

Но оказалось, что правильность концепции, профессионализм и мотивация участников Рабочей группы позволили не только найти финансирование для ключевых проектов Сейфнет в части «доверенной среды», мультимодальной биометрической идентификации или квантового распределения ключей, но и найти партнеров среди представителей властей крупного города федерального значения (СПб), крупных корпораций и регуляторов, которые существенно продвинули реализацию проектов Сейфнет в интересах других рынков НТИ и в интересах всей страны.